Black Duck Newsroom

Synopsys and Ponemon Release New Study Highlighting Software Security Practices and Challenges in the Financial Services Industry

Survey Conducted by Ponemon Institute Reveals More Than Half of Financial Services Organizations Have Experienced Theft of Customer Data Due to Insecure Software

Disclaimer: The Synopsys Software Integrity Group is now Black Duck®. Click here to learn more.

MOUNTAIN VIEW, Calif., Aug. 1, 2019 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released the report The State of Software Security in the Financial Services Industry. Based on a survey of global financial services organizations conducted by Ponemon Institute, the report highlights the industry's security posture and its ability to address security-related issues. The study found that more than half of the surveyed organizations have experienced theft of sensitive customer data or system failure and downtime because of insecure software or technology. The study also found that many organizations are struggling to manage cybersecurity risk in their supply chain and are failing to assess their software for security vulnerabilities before release.

"While the financial services industry is relatively mature in terms of their software security posture, organizations are grappling with a rapidly evolving technology landscape and facing increasingly sophisticated adversaries," said Drew Kilbourne, managing director of security consulting for the Synopsys Software Integrity Group. "There is no single right approach to software security, but this study clearly shows that there is a significant need for improvement in supply chain risk management. There is also an opportunity for many organizations to expand the scope of their software security programs to cover all their business-critical applications and shift their efforts further left in the software development life cycle (SDLC)."

Synopsys commissioned Ponemon Institute, a leading IT security research organization, to examine current software security practices and risks in the financial services industry (FSI). Ponemon surveyed over 400 IT security practitioners in various sectors of the financial services industry, including banking, insurance, mortgage lending/processing, and brokerage firms. The respondents' roles included development, installation, and implementation of applications for the financial services industry.

Key findings from the study include:

The majority of FSI organizations are ineffective at preventing cyberattacks. More than half of respondents have experienced system failure or downtime (56%) or theft of sensitive customer data (51%) due to insecure software or technology. Unsurprisingly, the study shows that more organizations are effective in detecting (56%) and containing (53%) cyberattacks than in preventing attacks (31%).

Many FSI organizations are struggling to manage cybersecurity risk in their supply chain. Nearly three-quarters (74%) of respondents were concerned or very concerned about the security posture of third-party software and systems. Despite this concern, only 43% of respondents said their organizations impose cybersecurity requirements on third parties involved in developing financial software and systems. Furthermore, only 43% of respondents said they have a formal process for inventorying and managing the open source code in

their software portfolios.

FSI organizations are failing to assess their software for security vulnerabilities before release. While most organizations follow a secure software development life cycle (SDLC) process, respondents reported that their organizations test, on average, only 34% of all financial software and technology developed or in use by their organization for cybersecurity vulnerabilities. For the software and technology that is tested for vulnerabilities, only 48% of respondents reported that security testing occurs in the pre-release phases of the SDLC, such as the requirements and design phase or the development and testing phase.

Download a free copy of the report: The State of Software Security in the Financial Services Industry

Register for the webinar on Sept. 12 at 1 p.m. ET.

Learn more about software security solutions for the financial services industry.

About the Synopsys Software Integrity Group

Synopsys Software Integrity Group helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle. Learn more at https://www.synopsys.com/software.

About Synopsys

Synopsys, Inc. (Nasdaq: SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. As the world's 15th largest software company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and is also growing its leadership in software security and quality solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest security and quality, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at https://www.synopsys.com/.

Editorial Contacts:
Mark Van Elderen
Synopsys, Inc.
650-793-7450
mark.vanelderen@synopsys.com

Liz Samet
Synopsys, Inc.
703-657-4218
elizabeth.samet@synopsys.com

SOURCE Synopsys, Inc.

---

https://news.blackduck.com/2019-08-01-Synopsys-and-Ponemon-Release-New-Study-Highlighting-Software-Security-Practices-and-Challenges-in-the-Financial-Services-Industry